Correspondence

The Separability of Standard Cyclic N-ary Gray Codes

A. J. van Zanten and I Nengah Suparta

***Abstract*—A Sharp lower bound is derived for the cyclic list distance between two codewords, having Hamming distance m, in the standard N-ary Gray code of length n, for $1 \le m \le n$ and for even values of N. The bound generalizes a similar result in the binary case.**

***Index Terms*—Cyclic code, Gray code, separability.**

I. Introduction

A binary Gray code of length n is an ordered sequence (*list*) of all 2^n n-bit strings (*codewords*) such that successive codewords differ in exactly one bit position. The best known example of such an ordered code is the *binary reflected Gray code* (cf., e.g., [8], [10] and also Section II), sometimes called *standard binary Gray code.* A question of theoretical as well as of practical relevance is the following. If two codewords in a Gray code, or in any ordered code, differ in m positions, how far are they separated from each other in the list of codewords? The larger this list distance of the code, the smaller the number of bit errors will be when transmitting codewords by means of analog signals (cf. [10]). Stated more precisely, when we index the codewords in the list from 0 until $2^n - 1$, and if two codewords $\underline{g}_i$ and $\underline{g}_j$ have Hamming distance $d_H(\underline{g}_i, \underline{g}_j) = m$, can we find a bounding function b such that the list distance satisfies $d_L(\underline{g}_i, \underline{g}_j) \ge b(m)$, for $1 \le m \le n$? Of course, the most interesting bounding function is a function giving sharp lower bounds for all values of m, i.e., such that for every m-value there exists at least one pair of codewords with list distance $b(m)$. The question of finding this uniquely determined function is called the *separability problem* (cf. [9], [10]). We shall use the term *separability function* for a function b—occasionally denoted as $b(m)$—yielding sharp lower bounds for $1 \le m \le n$. In [9], Yuen solves the separability problem for the binary standard Gray code. The separability function in this case appears to be $\lceil \frac{2^m}{3} \rceil$. The derivation of this expression is accomplished by making use of the *index system* of the standard Gray code, i.e., the relationship between a codeword $\underline{g}_i$ and its index i, $0 \le i \le 2^n - 1$ (cf. e.g. [8]). Along similar lines, Cavior in [1] derives a sharp upper bound for the list distance in this code, being $2^n - \lceil \frac{2^m}{3} \rceil$, $1 \le m \le n$. In both papers, the list of codewords is interpreted as a linear (noncyclic) list, which implies that $d_L(\underline{g}_i, \underline{g}_j)$ is defined as $|i - j|$. Now, it is well known that the standard Gray code is a *cyclic* Gray code, i.e., also the last codeword differs from the first one in precisely one bit position. Therefore, it is natural to introduce the *cyclic list distance* defined as

$$D\left(\underline{g}_i, \underline{g}_j\right) = \min\{|i - j|, 2^n - |i - j|\} \tag{1}$$

(cf. also [7]). With respect to this notion the results of Yuen and Cavior can be combined in the following implication

$$d_H\left(\underline{g}_i, \underline{g}_j\right) = m \rightarrow D\left(\underline{g}_i, \underline{g}_j\right) \ge \left\lceil \frac{2^m}{3} \right\rceil. \tag{2}$$

We call this implication the *separability property* of the standard binary Gray code.

Next we will derive a more general separability property which holds for the standard N-ary Gray code when N is even. Although an index system for this code is known (cf. [4]), it will appear that such a system is not needed to prove the result. Throughout this correspondence, the terms list and Gray code (which is represented by that list) are interchangeable. The columns of this list are numbered from right to left by $1, 2, \ldots, n$.

II. Preliminaries and Definitions

As is well known, an *N-ary Gray code* $N > 0$ of length n is an ordered list of all N^n codewords of length n over the set of integers $S = \{0, 1, \ldots, N - 1\}$, such that each codeword differs from the previous one in exactly one position. The natural number N is called the *radix* of the code (cf. [3]). The notion of N-ary Gray code is, of course, a generalization of a binary Gray code whose radix is equal to two. If also the last codeword of the list differs in one position from the first codeword, one speaks of a *cyclic* N-ary Gray code. In this case, the Hamming distance of any codeword to its two immediate neighbors in the list is equal to one, where the list is considered to be a cyclic list. More specifically, one can require that if $\underline{g}_i$ is the ith codeword in the list with coordinates $g_{ik} \in S$, $1 \le k \le n$, and if $\underline{g}_{i+1}$ differs from $\underline{g}_i$ only in the jth position, one either has $g_{i+1j} = g_{ij} + 1$ or $g_{i+1j} = g_{ij} - 1, \bmod N$, for all values of i with $0 \le i \le N^n - 1$. Such a code can be defined as a *minimal-change* N-ary Gray code. Here, we identify the codeword with index N^n with the codeword with index 0. One could also say that codewords which are neighbors in this list are at *Lee distance* 1 from each other, with respect to the ring $\boldsymbol{Z}_N$ (cf. [6, p. 1750]). In this correspondence, the term N-ary Gray code applies to this type of cyclic codes. If the above property only holds for $0 \le i < N^n - 1$, and not for $i = N^n - 1$, the code will be called a noncyclic N-ary Gray code.

A well-known N-ary Gray code is the *reflected N-ary Gray code* of length n, $n \in \boldsymbol{Z}^+$, denoted by $G(n, N)$, and recursively defined as

$$G(n, N) = \begin{pmatrix} 0 & G(n-1, N) \\ 1 & G(n-1, N)^R \\ 2 & G(n-1, N) \\ \vdots & \vdots \\ N-1 & G(n-1, N)^* \end{pmatrix}$$

$$G(1, N) = \begin{pmatrix} 0 \\ 1 \\ 2 \\ \vdots \\ N-1 \end{pmatrix} \tag{3}$$

where $G(n-1, N)^R$ denotes the list $G(n-1, N)$ in reversed ordered. The symbol $*$ stands for R only when N is even, otherwise it should be deleted. It will be obvious that $G(n, N)$ is a cyclic N-ary Gray code if N is even and a noncyclic N-ary Gray code if N is odd and larger than 1 (cf. [3]).

The code $G(n, N)$ will be called the *standard N-ary Gray code.* In the remaining part of this correspondence, we only consider even values of N.

Manuscript received February 26, 2002; revised August 24, 2002.

A. J. van Zanten is with the Delft University of Technology, Faculty of Information Technology and Systems, Department of Mathematics, 2600 GA Delft, The Netherlands (e-mail: A.J.vanZanten@twi.tudelft.nl).

I N. Suparta is with the Department of Mathematics, P.O. Box 5031, 2600 GA Delft, The Netherlands, on leave from the Department of Mathematics, IKIP Negeri Singaraja, Bali—Indonesia (e-mail: isuparta@yahoo.com).

Communicated by J. Justesen, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2002.807305

III. Equivalence of Ordered Codes

Let $V_{n,N}$ denote the set of all cyclic minimal-change N-ary Gray codes of length n. Let G be some code in $V_{n,N}$. We shall introduce a number of transformations mapping G to some other (possibly the same) element of $V_{n,N}$:

i) if p is a permutation of the integers $1, 2, \ldots, n,$ then pG is the code of length n obtained by permuting the columns of G according to p;

ii) if a is the cyclic permutation $(0, 1, 2, \ldots, N-1)$, then a_iG is the code of length n obtained by permuting the integers in the ith column according to a, for some $i \in \{1, 2, \ldots, n\}$;

iii) if b is the permutation $(0, N-1)(1, N-2) \cdots (\frac{N}{2}-1, \frac{N}{2})$, then b_iG is the code of length n obtained by permuting the integers in the ith column according to b, for some $i \in \{1, 2, \ldots, n\}$ (cf. [5] and also [2, Ch. 2]).

It will be clear that all these transformations define mappings of $V_{n,N}$ onto itself, and also that these transformations generate a group of order $n!(2N)^n$. (Observe that the permutations a and b generate the dihedral group D_N of order $2N$.) We remark that the subgroup generated by the transformations ii) is isomorphic to the translation group $G \rightarrow G+\underline{a}$, $\underline{a} \in S^n$. Furthermore, applying transformation iii) to column n in case of $G(n, N)$, yields the reversed code $G(n, N)^R$.

Definition 3.1: Codes which can be transformed into each other by applying one or more of the transformations i)–iii) are called equivalent codes.

The relevance of this definition will become clear from the following proposition.

Proposition 3.2: Equivalent codes satisfy the same separability property.

The proof is immediate by observing that Hamming distances and list distances are not affected by the transformations i)–iii).

IV. Contractions of Ordered Codes

Let G be some code in $V_{n,N}$. Take two k-strings

$$\underline{a} := a_1\, a_2 \cdots a_k \in S^k \quad \text{and} \quad \underline{i} := i_1\, i_2 \cdots i_k$$

with $1 \leq i_1 < i_2 < \cdots < i_k \leq n$, for some fixed k-value, $1 \leq k \leq n$. The string $\underline{a}$ will be called a *bit pattern* and $\underline{i}$ a *position vector*. We now consider the sublist of G consisting of all codewords which have a_j on position i_j, for $1 \leq j \leq k$. Leaving out the common bit pattern $\underline{a}$ from these codewords provides us with an ordered code of codeword length $n-k$. We call this code the *contraction* of G with respect to the pair $(\underline{a}, \underline{i})$, and we write $G(\underline{a}, \underline{i})$. In particular, we can contract the standard N-ary Gray code $G(n, N)$ with respect to some pair $(\underline{a}, \underline{i})$. The resulting code will be denoted by $G(n, N; \underline{a}, \underline{i})$.

Proposition 4.1: Let $G(n, N)$ be the standard N-ary Gray code, $n > 1$, and let N be even. Then for any pair $(\underline{a}, \underline{i})$, the contraction $G(n, N; \underline{a}, \underline{i})$ is a cyclic Gray code equivalent to the standard Gray code $G(n-k, N)$.

Proof: Since N is even, $G(n, N)$ is cyclic. We shall prove the proposition by applying mathematical induction to n.

a) The statement is true for $n = 2$, as can be verified by inspection.

b) Assume the statement holds for all codeword lengths less than n. Consider the sublist of all codewords of $G(n, N)$ containing pattern $\underline{a}$ on position $\underline{i}$. If $i_k = n$, this sublist is either part of a sublist $a_nG(n-1, N)$ or of a sublist $a_nG(n-1, N)^R$. In the first case, the code $G(n-k, N; \underline{a}, \underline{i})$ can be considered as the contraction $G(n-1, N; \underline{a}', \underline{i}')$, with $\underline{a}' = a_1a_2 \cdots a_{k-1}$ and $\underline{i}' = i_1\, i_2 \cdots i_{k-1}$. By the induction assumption, this last code is equivalent to $G(n-1-k+1, N) = G(n-k, N)$. In the second case, we proceed similarly, making use of the equivalence of $G(n-k, N)$ and $G(n-k, N)^R$ (cf. the remark prior to Definition 3.1). If $i_k \neq n$, the contraction process yields a code of type

$$G(n, N; \underline{a}, \underline{i}) = \begin{pmatrix} 0 & G(n-1, N; \underline{a}, \underline{i}) \\ 1 & G(n-1, N; \underline{a}, \underline{i})^R \\ 2 & G(n-1, N; \underline{a}, \underline{i}) \\ \vdots & \vdots \\ N-1 & G(n-1, N; \underline{a}, \underline{i})^R \end{pmatrix}.$$

Again, by the induction assumption $G(n-1, N; \underline{a}, \underline{i})$ is equivalent to the standard code $G(n-1-k, N)$. Applying Definition 3.1 shows that $G(n, N; \underline{a}, \underline{i})$ is equivalent to $G(n-k, N)$. □

V. Separability of the Standard N-ary Gray Code

We are ready now to prove our main result.

Theorem 5.1: Let $G(n, N)$ be the standard N-ary Gray code of length n, and let N be even. If the Hamming distance between two codewords $\underline{g}$ and $\underline{h}$ satisfies $d_H(\underline{g}, \underline{h}) = m$, then the list distance between $\underline{g}$ and $\underline{h}$ satisfies $D(\underline{g}, \underline{h}) \geq \lceil \frac{N^m}{N^2-1} \rceil$. Moreover, this lower bound is sharp for all m-values with $1 \leq m \leq n$.

Proof: We prove the theorem in two steps.

A) First we take $m = n$. In addition to the statement of the theorem, we shall also prove that there is a pair of codewords at minimum distance, such that the shortest path connecting them in the list $G(n, N)$ contains the first codeword as well as the last codeword of the list (3). For $n = 1$ and $n = 2$, all above statements are trivial. Assume all these statements are true for all values less than $n > 2$. Let $\underline{g}$ and $\underline{h}$ be two codewords with $d_H(\underline{g}, \underline{h}) = n$. If we write $\underline{g} = g_n g_{n-1} \underline{v}$ and $\underline{h} = h_n h_{n-1} \underline{w}$, it follows that $g_n \neq h_n$, $g_{n-1} \neq h_{n-1}$ and $d_H(\underline{v}, \underline{w}) = n-2$. From (3), it follows that $\underline{v}$ and $\underline{w}$ can be considered as codewords of $G(n-2, N)$ or of $G(n-2, N)^R$. It also follows that $\underline{g}$ and $\underline{h}$ are separated from each other by at least a number $p (\geq 1)$ of complete blocks $G(n-2, N)$ or $G(n-2, N)^R$ of size N^{n-2}. So $D(\underline{g}, \underline{h})$ is equal to pN^{n-2} plus a term due to the positions of $\underline{v}$ and $\underline{w}$ in their respective blocks $G(n-2, N)$ or $G(n-2, N)^R$. It will be obvious that $D(\underline{g}, \underline{h})$ is minimal if both contributions can be minimized simultaneously. This is indeed possible by taking $p = 1$ and by selecting codewords $\underline{v}$ and $\underline{w}$, which are both in a block $G(n-2, N)$ or both in a block $G(n-2, N)^R$ for odd p-values, as described in the beginning of this proof. Due to the induction assumptions $D(\underline{g}, \underline{h})$ is minimal for this choice of $\underline{v}$ and $\underline{w}$ and its value is equal to

$$N^{n-2} + \left\lceil \frac{N^{n-2}}{N^2-1} \right\rceil = \left\lceil \frac{N^n}{N^2-1} \right\rceil.$$

Therefore, the theorem also holds for n. In particular, we can take $\underline{g} = \underline{0}$ and $\underline{h} = c\ 1\ c\ 1\ c \cdots$, with $c = N-1$, showing that also the additional induction requirement is satisfied again. By the principle of mathematical induction, the theorem has been proved now for the case $m = n$.

B) If $m < n$, then $\underline{g}$ and $\underline{h}$ are equal in $k := n-m$ positions, indicated by some position vector $\underline{i} = i_1, i_2, \ldots, i_k$. The corresponding values of the coordinates will be given by $\underline{a} = a_1, a_2, \ldots, a_k$. Now, we consider the contraction

$G(n, N; \underline{a}, \underline{i})$. Let $\underline{v}$ and $\underline{w}$ be the codewords in this contraction which correspond to $\underline{g}$ and $\underline{h}$, respectively. So, we have $d_H(\underline{v}, \underline{w}) = m$. Since $G(n, N; \underline{a}, \underline{i})$ is equivalent to $G(m, N)$, it follows, by Proposition 3.2 and part A of this proof, that $D(\underline{v}, \underline{w}) \geq \lceil \frac{N^m}{N^2-1} \rceil$ in the contracted code. Hence, we have *a fortiori* the same inequality for $D(\underline{g}, \underline{h})$, since in $G(n, N)$ the codewords corresponding to codewords of $G(n, N; \underline{a}, \underline{i})$ will, in general, be interlaced by codewords which have no counterpart in $G(n, N; \underline{a}, \underline{i})$. Finally, one can easily prove that this bound is sharp by applying mathematical induction to $n \geq m$, and using part A for the case $n = m$. □

Corollary 5.2 (Yuen, Cavior): The separability function of the standard binary Gray code is equal to $\lceil \frac{2^m}{3} \rceil$.

References

[1] S. R. Cavior, "An upper bound associated with errors in Gray code," *IEEE Trans. Inform. Theory*, vol. IT-21, p. 596, Sept. 1975.

[2] M. Cohn, "Affine m-ary Gray codes," *Inform. Contr.*, vol. 6, pp. 70–78, 1963.

[3] M. C. Er, "On generating the N-ary reflected Gray codes," *IEEE Trans. Computers*, vol. C-33, pp. 739–741, Aug. 1984.

[4] I. Flores, "Reflected number system," *IRE Trans. Electron. Computer*, vol. EC-5, pp. 79–82, 1956.

[5] E. N. Gilbert, "Gray codes and paths on the n-cube," *Bell Syst. Tech. J.*, vol. 37, pp. 815–826, 1958.

[6] V. S. Pless and W. C. Huffman, Eds., *Handbook of Coding Theory*. Amsterdam, The Netherlands: Elsevier, 1998.

[7] F. P. Preparata and J. Nievergelt, "Difference-preserving codes," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 643–649, Sept. 1974.

[8] E. M. Reingold, J. Nievergelt, and N. Deo, *Combinatorial Algorithms: Theory and Practice*. Englewood Cliffs, NJ: Prentice-Hall, 1977.

[9] C. K. Yuen, "The separability of Gray code," *IEEE Trans. Inform. Theory*, vol. IT-20, p. 668, Sept. 1974.

[10] A. J. van Zanten, "Index system and separability of constant weight Gray codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1229–1233, July 1991.

Disproof of a Conjecture on the Existence of Balanced Optimal Covering Codes

Patric R. J. Östergård, *Senior Member, IEEE*

***Abstract*—The minimum number of codewords in a binary code with length n and covering radius R is denoted by $K(n, R)$, and corresponding codes are called optimal. A code with M words is said to be balanced in a given coordinate if the number of 0's and 1's in this coordinate are at least $\lfloor M/2 \rfloor$. A code is balanced if it is balanced in all coordinates. It has been conjectured that among optimal covering codes with given parameters there is at least one balanced code. By using a computational method for classifying covering codes, it is shown that there is no balanced code attaining $K(9, 1) = 62$.**

***Index Terms*—Balanced code, code equivalence, covering code.**

Manuscript received June 6, 2001; revised September 10, 2002. This work was supported by the Academy of Finland under Grants 44517 and 100500.

The author is with the Department of Electrical and Communications Engineering, Helsinki University of Technology, 02015 HUT, Finland (e-mail: patric.ostergard@hut.fi).

Communicated by S. Litsyn, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2002.807307

I. Introduction

We consider binary codes, $C \subseteq F^n$ where $F = \{0, 1\}$, and denote such a code of length n, cardinality M, and covering radius R by $(n, M)R$. Given n and R, we denote the least integer M such that an $(n, M)R$ code exists by $K(n, R)$, and call $(n, K(n, R))R$ codes *optimal*. A complete survey of all aspects of covering codes can be found in [2].

The concept of *balanced* codes was introduced in [3]. A binary code of size M is said to be balanced in a given coordinate if the number of 0's and 1's in this coordinate are at least $\lfloor M/2 \rfloor$. A code is balanced if it is balanced in all coordinates. The following conjecture is stated in [3]; see also [2, p. 149].

Conjecture. Among all optimal covering codes with given parameters, at least one is balanced.

If the Conjecture would turn out to be true, it could be utilized in the search for optimal covering codes. Clearly, there are optimal codes that are not balanced, for example, the optimal $(2, 2)1$ code $\{00, 01\}$. The Conjecture, however, only claims that there exists a balanced code. Indeed, there exists a balanced $(2, 2)1$ code: $\{00, 11\}$.

The size of optimal binary codes has been determined in the following cases [3], [4], [7], [9], [10]: for perfect codes, for codes with length at most 9, for codes with size at most 7, and for codes with covering radius 1 whose length exceeds that of Hamming codes by 1. Among these, balanced optimal codes are known for all other cases but $(9, 62)1$ codes (using the classification in [9], [10] and direct combinatorial arguments).

A disproof must therefore be looked for among codes with length at least 9. Recently, the result $K(9, 1) = 62$ was obtained in a CPU-extensive computational proof by showing nonexistence of $(9, 61)1$ codes [7]. Two inequivalent $(9, 62)1$ codes have been published in the literature: the codes in [8] and [12] are balanced in five and six coordinates, respectively, and in the rest of the coordinates the number of 0's and 1's is 30 and 32 (or vice versa). Consequently, this seemed to be a possible instance for disproof of the Conjecture. Indeed, as we shall see in Section II of this correspondence, there exists no balanced $(9, 62)1$ code.

II. The Disproof

The computational method used in this work is from [7], which, in turn, was developed from ideas in [1], [5], [11]. The basic idea of the method is to construct an $n \times M$ matrix with the codewords as columns, row by row. The search is pruned by using linear inequalities that follow from the sphere-covering bound, by carrying out equivalence tests on subcodes, and by assuming that no codeword occurs more than once in the final code. We do not go into details here but refer the reader to [7].

In the search for balanced codes, we have the additional requirement that the number of 0's and 1's in each row (coordinate) be at least $\lfloor M/2 \rfloor$. This is easily implemented in the existing algorithm from [7].

Even if a classification of balanced codes is orders of magnitude faster than a complete classification, the computation took about one month of CPU time on 500-MHz PCs. The search was completed in a few days by distributing it over a local network using the distributed batch system autoson [6]. The number of inequivalent codes with $1 \leq n' \leq 9$ (corresponding to $n' \times 62$ matrices) is 1, 5, 30, 1068, 200 527, 13 123 199, 435 424, 45 718, 0, respectively, where the last number disproves the Conjecture.

It would still be interesting to know whether there exist counterexamples for $R > 1$.